Kentucky.gov

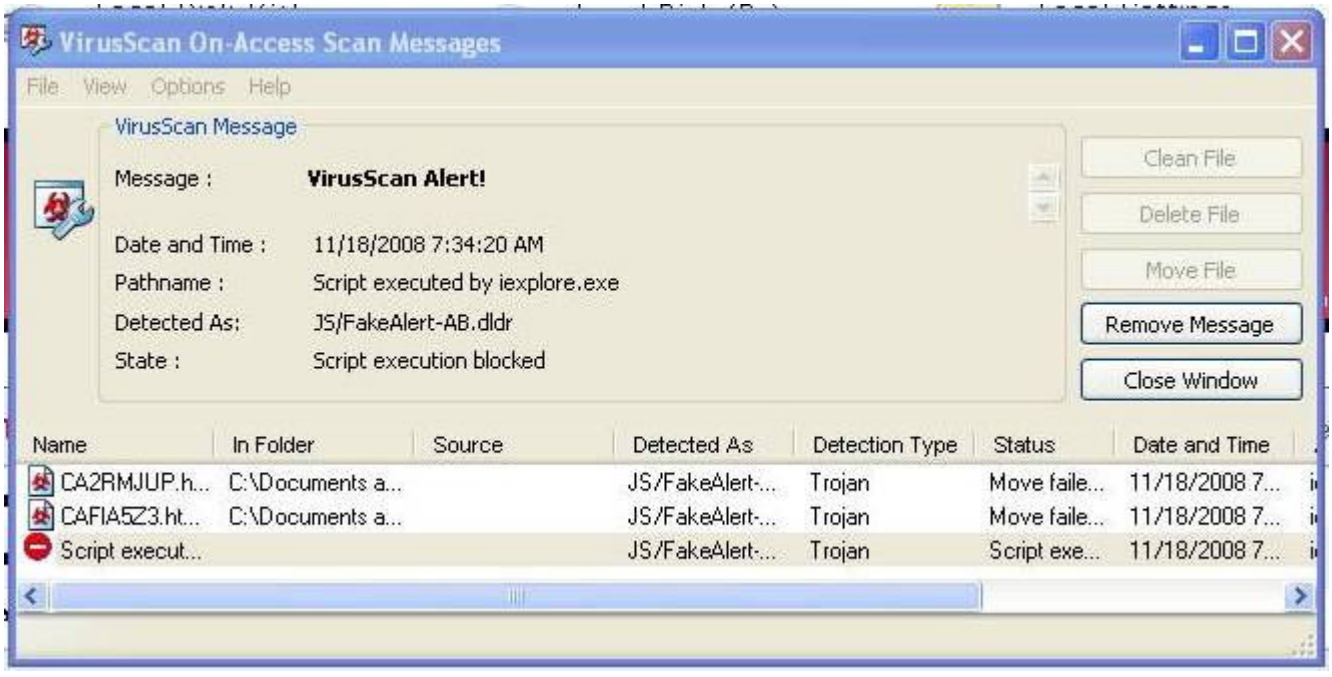
Commonwealth Office of Technology

From: Ritchey, Gail (COT)
Sent: Wednesday, November 19, 2008 1:44 PM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: COT Security Alert - JS.FakeAlert-AB Outbreak

COT Security Alert - JS.FakeAlert-AB Outbreak

The COT Security Administration has become aware of an outbreak of the **JS.FakeAlert-AB.dldr** virus which is becoming prevalent on the state network. The infection occurs when infected web pages visited by a user redirect the user to another site where malicious software is downloaded. All of this is completely automatic, with no action required by the user once an infected web page is accessed. Once the file is downloaded and attempts to run, a VirusScan Alert such as the one below may pop up. When this happens the machine is infected and must be updated, scanned and cleaned. Execution of the virus may be stopped by McAfee, but the downloaded file can be difficult to remove.

All occurrences of infection must be reported and remediated. Users at COT and its consolidated agencies should report occurrences of infection to the Commonwealth Service Desk, 502-564-7576 by phone and CommonwealthServiceDesk@ky.gov by email.



For the most effective antivirus scanning, cleaning and updating and a safer network environment, workstations must be powered on and users logged off when scheduled antivirus scanning takes place. The policy of COT and its consolidated agencies is that workstations are powered off only over weekends, and powered on but logged off on weeknights. This information may be found in section 7.2.0 of the Security Standard Procedures Manual at http://technology.ky.gov/security/sspm_toc.htm. Selecting either Log Off or Restart from the Shut Down menu at the end of each workday except Friday and choosing Shut Down on Friday will accomplish these results. Simply locking the workstation leaves applications open and the antivirus is not able to clean or remove all malicious files. Shutting down completely every night causes the machine to scan when it is powered back on and may cause an inefficient scan along with a noticable slowing of processes until the scan is complete.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/security/